REMARKS

STATUS OF CLAIMS

Claims 21, 23, 34, 37 and 41-44 have been amended.

Claim 45 has been added.

Claims 24 and 38 have been canceled.

Claims 21-23, 25-37 and 39-45 are currently pending in the application

ISSUES NOT RELATED TO PRIOR ART

35 U.S.C. § 112

Claims 21, 34 and 41-44 were previously rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention "because of the claim limitation establishing the secure connection between the first network device and the second network device based on the third description of network traffic."

"The Examiner's focus during examination of claims for compliance with the requirement for definiteness... is whether the claim meets the threshold requirements of clarity and precision, not whether more suitable language or modes of expression are available." MPEP §2173.02.

Applicant points the Examiner to the last paragraph of page 1 of the Specification, which reads, in pertinent part:

> In certain embodiments of the invention, **the source end host and the initiator peer may be one device**, such as a router or switch executing an IPSec agent. Similarly, **the destination end host and the responder peer may be one device**.

From this language, one skilled in the art could easily determine whether the connection between the first network device and the second network device could be established or not. Because the source end host and the initiator peer may be one device, as well as the destination end host and the responder peer, the secure connection may be established between the first network device and the second network device.

Applicant has added Claim 45 to further clarify this issue. New Claim 45 reads:

> The apparatus of Claim 34, wherein:
> said first network device comprises a first endpoint host associated with the first network device; and
> said second network device comprises a second endpoint host associated with the second network device.

The Specification clearly states that the source end host and destination end host may be communicatively coupled to the initiator peer and responder peer, respectively, as well as the embodiment described above wherein the source end host and the initiator peer may be one device, as well as the destination end host and the responder peer.

Applicant believes that the above clarification, as well as the newly added claim, is sufficient to overcome the rejection, and Applicant respectively requests withdrawal of the rejection.

ISSUES RELATING TO PRIOR ART

A. CLAIMS 21-44 -- 35 U.S.C. § 103(a)

Claims 21-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,823,462 to Cheng et al. (hereinafter *Cheng*) in view of U.S. Patent No. 5,968,176 to Nessett et al. (hereinafter *Nessett*). The rejections are respectfully traversed.

Claims 21-44 are allowable over the cited reference because each of claims 21-44 contains at least one element that is not disclosed, taught, or suggested by the cited reference, the cited reference has not been properly combined with any other reference, and the Office Action fails to demonstrate a suggestion to combine.

As stated in the Federal Circuit decision *In re Dembiczak*, 50 USPQ.2d 1617 (Fed. Cir. 1999), (citing *Gore v. Garlock*, 220 USPQ 303, 313 (Fed. Cir. 1983)), "it is very easy to fall victim to the insidious effect of the hindsight syndrome where that which only the inventor taught is used against its teacher." *Id.* The Federal Circuit stated in *Dembiczak* "that the best defense against subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for a showing of the teaching or suggestion to combine prior art references." *Id.* Thus, the Federal Circuit explains that a proper obviousness analysis requires "***particular factual findings*** regarding the locus of the suggestion, teaching, or motivation to combine prior art references." *Id.* (emphasis added).

> In particular, the Federal Circuit states:
> "We have noted that evidence of a suggestion, teaching, or motivation to combine may flow from the prior art references themselves, the knowledge of one of ordinary skill in the art, or, in some cases, from the nature of the problem to be solved...although 'the suggestion more often comes from the teachings of the pertinent references'...The range of sources available, however, does ***not diminish the requirement for actual evidence***. That is, the ***showing must be clear and particular***...Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence.'" *Id.* (emphasis added; internal citations omitted).

Neither *Cheng* nor *Nessett* show any suggestion, teaching, or motivation to combine their teachings, nor does the Office Action provide a "clear and particular" showing of the suggestion, teaching, or motivation to combine their teachings. In fact, the only motivation provided in the Office Action is the hindsight observation that by combining features of those references, one may achieve the benefits achieved from the invention as described and claimed in the application. Such a hindsight observation is not consistent with the Federal Circuit's requirement for "particular factual findings."

With respect to Claim 21, the Office Action alleges that *Cheng* shows all of the limitations of Claim 21 except for "disclos[ing] expressly the first description comprises a first set of network addresses." The Office Action goes on the state that it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine "the teaching of *Nessett* within the system of *Cheng* because (a) *Cheng* teaches a security policy in a virtual private network to establish a secure tunnel and (b) *Nessett* teaches enhanced security features that can be distributed in multiple layers to multiple devices, and managed using a coherent security policy management interface to provide end-to-end protection of tunnels between intermediate routers as well as between a router and an end-system." (internalcitations omitted)

However, none of the above alleged features of *Nessett* are relevant to the **claimed** features. It is unclear how "enhanced security features that can be distributed in multiple layers to multiple devices, and managed using a coherent security policy management interface to provide end-to-end protection of tunnels between intermediate routers as well as between a router and an end-system" teaches a first description of network traffic that comprises a first set of netowkr addresses.

As discussed in prior communications, *Cheng* is directed to an approach for determining a security policy in a virtual private network where the endpoints of the tunnel are **known**. *Cheng* is concerned with how traffic between known endpoints is to be protected, not about determining which endpoints should have security policies applied. This is clear from the following language in *Cheng*:

> In step 330, a tunnel definition database in the server node 110A is configured so that the server node 110A has one tunnel definition for each of the plurality of tunnels 120 associated with a group name. As stated in the Background Information section, the tunnel definition establishes the end points of that particular tunnel 120.

Cheng, col. 5, lines 62-67.

There is nothing in *Cheng* that teaches, anticipates or suggests an approach for determining which end hosts should have security applied to them. The clear novelty of one of the claimed approaches is that hosts unknown to one endpoint may be determined to be secure. One example is that the claimed approach allows a host to securely communicate with a private address, such as private addresses behind a NAT or non-exposed hosts behind a firewall.

In the same vein, *Nessett* teaches establishing security functions in a network **where all hosts and data paths are known**. The following language from *Nessett* makes this abundantly clear:

> The system includes a topology data store, that stores information about security functions operating in the set of nodes in the network, and **about interconnection of nodes in the network**. (col. 4, lines 7-10)
>
> Further,
>
> The topology data store in one preferred aspect includes **data structures that provide information about particular nodes in the set of nodes that fall within the security framework**. The data structures include information such as network layer addresses, MAC layer addresses, higher layer user identifiers, transport layer port and socket numbers, whether or not a particular node is trusted to enforce security policy, the type of security policy that the node is able to enforce, the constructs used to enforce policy, the format of configuration data required for the security constructs, **and the connections of the node to other nodes in the network**. (col. 5, lines 27-38)

It is unclear how there could exist a motivatation to combine the references when neither reference suggests the approach addressed by the claimed features.

Further, neither *Cheng* nor *Nessett* anticipates, teaches or suggests "creating and storing a third description of network traffic that is to be protected based on determining a logical intersection of the first description of network traffic and the second description of network traffic, wherein the step of creating and storing a third description further comprises the step of determining a largest common subset between the first set of network addresses and the second set of network addresses; and establishing the secure connection between the first network device and the second network device based on the third description of network traffic."

This is shown by, among other things, *Cheng* specifically discussing the use of IKE Phase 2:

> As stated above, IKE is used to establish security associations in order to activate a particular tunnel 120. IKE is made up of two phases defined within an Internet Security Association and Key Management Protocol (ISAKMP) framework. The ISAKMP framework establishes the security associations and cyrptographic keys. The first phase establishes the security associations between the plurality of nodes 110 establishing a particular tunnel. IKE assumes that no secure channel, i.e., tunnel, currently exists and therefore it must initially establish one to protect any ISAKMP messages. The second phase refers to the negotiation of the security association for Internet Protocol (IP) security. Upon the successful completion of the negotiation of the phase two security association, data may be transferred between the plurality of nodes 110 establishing the tunnel 120. (col. 7, lines 16-30)

This actually teaches away from the claimed approaches, because IKE tunnels have known endpoints. There is no suggestion in *Cheng* for a secure connection to be established based upon a largest common subset of network addresses, because the network addresses of the endpoints are already known. The claimed approach is not negotiating how the data is to be transferred, as opposed to *Cheng.*

In *Nessett*, the only sections cited in the Office Action regarding this feature are:

> [W]hether or not it is trusted to enforce security policy, what type of enforcement rules it is capable of enforcing, the formats of security constructs in the node, and its interconnection among nodes in the network. (col. 6, lines 62-65)

And:

> wherein the security functions operating in the plurality of network device types across multiple protocol layers are coordinated by the security policy so that particular device types enforce the part of the security policy pertinent to the associated part of the network. (col. 24, lines 48-52)

In no way do the cited sections teach, suggest or disclose the featured "creating and storing a third description further comprises the step of determining a largest common subset between the first set of network addresses and the second set of network addresses; and establishing the secure connection between the first network device and the second network device based on the third description of network traffic."

There is no motivation in *Nessett* for a secure connection to be established based upon a largest common subset of network addresses, because the network addresses of the endpoints are already known, in addition to the security to be applied for each node. This **specifically** teaches away from the claimed novelty.

Solely in order to expedite positive resolution of the case and place the case in condition for allowance, Claims 21, 34 and 41-44 have been amended to incorporate the features of dependent Claim 24, which read:

> wherein the first description **comprises a packet summary value that summarizes packets in the network traffic to be protected**, and wherein the second description is generated by the second network device **based on comparing the packet summary value to one or more access control lists that are managed by the second network device**.

With respect to Claim 24, the Office Action alleges that *Cheng* as modified by *Nessett* teaches the claimed features. The only support for this in the Office Action are a nonexistent Fig. 14 and the following section from *Cheng*:

> The responding node 110 transfers its security policy to the initiator node 110 in the second message if the security policy of the responding node 110 matches the security policy of the initiator node 110. In another embodiment, the responding node 110 transfers its security policy to the initiator node 110 in the second message if both nodes 110 agree on the same set of protection suites in their security policy at any point in time. Additionally, cookies are generated to incorporate into the ISAKMP header in the first and second message. Cookies ensure protection against denial of service attacks and the pair of cookies (the initiator's cookie and responder's cookie) identify the ISAKMP security association. (col. 7, lines 46-57)

Nowhere in the above passage is any teaching, suggestion or disclosure of a first description of network traffic that **comprises a packet summary value that summarizes packets in the network traffic to be protected**, and wherein the second description is generated by the second network device **based on comparing the packet summary value to one or more access control lists that are managed by the second network device**.

The Office Action appears to attempt to argue inherency ("security policy must fundamentally include access control rules"), but there is no explantion or support given. Further, there is no mention or suggestion of a packet summary in the cited language.

Independent Claims 34 and 41-44 include the same features discussed above for Claim 21 that are lacking from the cited references. Therefore, Claims 34 and 41-44 are allowable for the same reasons given above for Claim 21.

Each of the dependent claims depend directly or indirectly on one of the independent claims that includes the features listed above for Claim 21. Therefore, each of the dependent claims are patentable for the same reasons set forth above with respect to Claim 21. In addition, each of the dependent claims feature other subject matter that independently render them patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully Submitted,

HICKMAN PALERMO TRUONG &
BECKER LLP

Date: October 26, 2006

Stephen J. Shaw
Reg. No. 56,442

(408) 414-1080, Ext. 231
Fax: (408) 414-1076
2055 Gateway Place, Suite 550
San Jose, CA 95110-1089

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop RCE, P.O. Box 1450, Alexandria, VA 22313-1450.

on October 26, 2006 by Stephen J. Shaw